



中华人民共和国国家标准

GB/T 45906.4—2025

变电站二次系统 第4部分：网络安全防护

Substation secondary system—Part 4: Cyber security protection

2025-08-01 发布

2026-02-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 总则 2

 5.1 防护原则 2

 5.2 防护体系 2

6 安全防御 3

 6.1 基础设施安全 3

 6.2 网络结构安全 3

 6.3 网络边界安全 3

 6.4 本体安全 4

 6.5 作业操作安全 7

 6.6 可信安全免疫 7

7 安全监测 8

 7.1 基本要求 8

 7.2 采集 8

 7.3 存储 8

 7.4 分析 8

 7.5 告警 8

8 安全处置 9

9 安全评估 9

 9.1 安全核查 9

 9.2 安全评价 9

附录 A（资料性） 变电站二次系统面临的主要网络安全威胁 10

参考文献 11

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 45906《变电站二次系统》的第4部分。GB/T 45906 已经发布了以下部分：

- 第1部分：通用要求；
- 第2部分：数据与模型；
- 第3部分：通信报文规范；
- 第4部分：网络安全防护；
- 第5部分：保护控制及相关设备；
- 第6部分：站内监控系统；
- 第7部分：集中监控系统；
- 第8部分：电气操作防误；
- 第9部分：建设规范；
- 第10部分：试验与检测。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国电力企业联合会提出。

本文件由全国电网运行与控制标准化技术委员会(SAC/TC 446)、全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本文件起草单位：国家电力调度控制中心、国网上海市电力公司、南京南瑞信息通信科技有限公司、中国电力科学研究院有限公司、国网湖北省电力有限公司、国网北京市电力公司、国网江西省电力有限公司、国网宁夏电力有限公司、国家电网有限公司西北分部、国网河北省电力有限公司、国网江苏省电力有限公司、国网河南省电力公司、国网青海省电力公司、中国南方电网有限责任公司、南京南瑞继保电气有限公司、北京科东电力控制系统有限公司、国电南瑞科技股份有限公司、北京四方继保工程技术有限公司、许继电气股份有限公司、国电南京自动化股份有限公司、国网经济技术研究院有限公司、北京同创安全可信科技有限公司。

本文件主要起草人：周劼英、王治华、张晓(国家电力调度控制中心)、李明节、周泽昕、舒治淮、詹雄、朱江、邵立嵩、吕鹏飞、刘宇、金龙、杨维永、汤震宇、刘苇、张晓(湖北)、张宏杰、高鑫、韩盟、栗维勋、陈明亮、余璟、王丹、李延和、林青、宁志言、沈艳、贾玲、马斌、吴金宇、仇伟杰、张龙、王旭宁、汤成俊、沈志浩、余越、李仲青、朱朝阳、李劲松、孟江雯、卢曦、高明慧、王鹏、常家乐、孙瑜、刘长卿。

引 言

为满足变电站二次系统转型发展需求,实现变电站二次系统整体架构、功能、数据、设备的顶层设计,助推新型电力系统设备制造产业优化升级,提升变电站二次系统整体性能和可靠性水平,制定本系列标准。

GB/T 45906《变电站二次系统》从通用需求、设备系统功能需求和工程实施与检测等方面全面涵盖了变电站二次系统各环节,拟由 10 个部分构成。

- 第 1 部分:通用要求。目的在于规范变电站二次系统总体要求和可靠性、功能集成、信息交互、网络安全等技术要求。
- 第 2 部分:数据与模型。目的在于规范变电站二次系统数据和模型框架,明确数据分类、采集处理要求、建模方法和模型配置流程。
- 第 3 部分:通信报文规范。目的在于规范变电站二次系统的通信协议集,明确数据对象和通信服务的实现方法。
- 第 4 部分:网络安全防护。目的在于规范变电站二次系统安全防护的技术要求。
- 第 5 部分:保护控制及相关设备。目的在于规范变电站继电保护及安全自动装置、自动化设备、电能计量及电能质量设备、采集执行设备、通信设备及辅助监控设备等的技术要求。
- 第 6 部分:站内监控系统。目的在于规范站内监控系统的功能、性能、信息交互等技术要求。
- 第 7 部分:集中监控系统。目的在于规范变电站集中监控系统的系统架构、功能、性能、信息交互等技术要求。
- 第 8 部分:电气操作防误。目的在于规范变电站二次系统电气操作防误的总体要求、架构、功能、性能及应用要求。
- 第 9 部分:建设规范。目的在于规范变电站二次系统工程建设的总体要求、设计原则、过程控制和技术要求。
- 第 10 部分:试验与检测。目的在于规范变电站二次系统设备和系统的检测总体原则、检测要求等。

变电站二次系统

第4部分：网络安全防护

1 范围

本文件规定了变电站二次系统网络安全防护的总则、安全防御、安全监测和安全评估。
本文件适用于变电站二次系统网络安全设施的设计、研发、采购、部署、维护、评估等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 36572—2018 电力监控系统网络安全防护导则

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 cyber security

通过采取必要措施,防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。

注:网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

[来源:GB/T 22239—2019,3.1,有修改]

3.2

本体安全 self security

变电站二次系统各模块自身的安全、可控,包括业务系统软件的安全、操作系统和基础软件的安全、计算机和变电站二次设备的安全等。

[来源:GB/T 36572—2018,3.9,有修改]

3.3

可信安全免疫 trust security immunology

基于可信计算技术实现变电站二次系统的安全免疫,保障操作系统和业务系统软件安全可信,防范已知和未知的病毒、木马及恶意代码的侵害。

[来源:GB/T 36572—2018,3.10,有修改]

3.4

可信根实体 entity of root of trust

用于支撑可信计算平台信任链建立和传递的可对外提供完整性度量、安全存储、密码计算等服务的功能模块。

注：可信根实体包括可信平台控制模块(TPCM)、可信密码模块(TCM)、可信平台模块(TPM)等。

[来源：GB/T 37935—2019, 3.12]

4 缩略语

下列缩略语适用于本文件。

APT:高级持续威胁(Advanced Persistent Threat)

CPS:信息物理系统(Cyber Physical Systems)

GOOSE:通用面向对象的变电站事件(Generic Object Oriented Substation Event)

IP:网际互连协议(Internet Protocol)

MAC:媒体存取控制位址(Media Access Control Address)

PMU:同步相量测量装置(Phasor Measurement Unit)

5 总则

5.1 防护原则

结合变电站二次系统面临的网络安全威胁(见附录 A),网络安全防护宜遵循以下原则。

- a) 综合防护。在“安全分区、网络专用、横向隔离、纵向认证”基本防护策略的基础上,变电站二次系统从物理、网络、主机、终端、应用、数据、业务等多个层面,采用安全防护、安全监测、安全处置、安全评估等多种技术手段进行综合防护。
- b) 协同防护。变电站二次系统的网络安全作为电力监控系统整体网络安全防护体系的一部分,与所关联的其他系统相互配合,相互协作,构建协同安全防护体系。
- c) 动态防护。变电站二次系统根据所面临的安全威胁态势进行安全防御、安全监测等措施的适应性调整,形成动态的安全防护机制,及时有效地防范安全风险。
- d) 适当防护。变电站二次系统网络安全防护措施与业务系统有机融合,具备大范围推广价值和可靠实用效果,适应不同电压等级、不同类型变电站的实际业务需要。

5.2 防护体系

变电站二次系统应采用多种安全防护措施,构建“安全防御—安全监测—安全处置—安全评估”的网络安全防护体系,并具备动态提升网络安全防护的能力,如图 1 所示。其中,安全防御包括基础设施安全、网络结构安全、网络边界安全、本体安全、作业操作安全、可信安全免疫,安全监测包括对安全状态、安全事件进行采集、存储、分析、告警等处理,安全处置包括对日常告警进行处置的常态响应、在突发事件下执行网络安全应急预案执行和应急处置的应急响应,安全评估指对二次系统的安全防御、安全监测、安全处置的能力和状态进行安全核查和安全评价。

注：安全防御是整个体系的技术基础,安全监测是用于感知安全防御的状态,安全处置是对安全监测的响应。安全评估验证安全防御、安全监测和安全处置的有效性,指导各环节能力的持续提升。

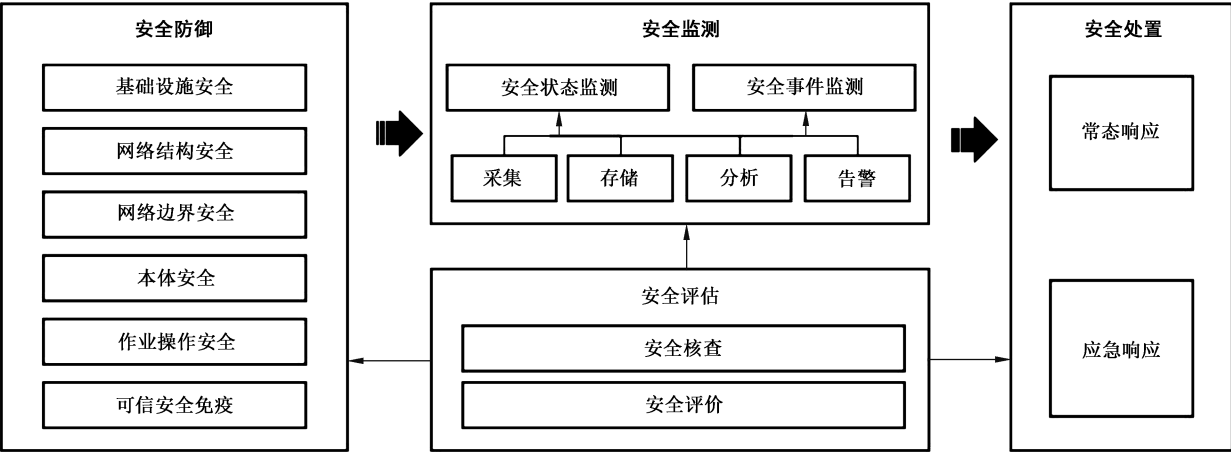


图 1 变电站二次系统防护体系示意图

6 安全防护

6.1 基础设施安全

变电站二次系统的基础设施安全应满足以下要求：

- a) 变电站二次系统所在的机房和生产场地满足 GB/T 36572—2018 中 6.1 的要求和 GB/T 22239 中的安全物理环境的要求；
- b) 辅助监控设备等部署在室外的设施采取防破坏措施、视频监控等技术手段加强物理空间防护；
- c) 支撑变电站二次系统的卫星时间同步系统采取防干扰、抗欺骗安全防护和隔离措施，具备常规电磁干扰信号入侵监测能力和实时告警能力；
- d) 生产控制区所有的密码基础设施通过国家密码主管部门的检测认证。

6.2 网络结构安全

变电站二次系统的网络结构安全满足以下要求：

- a) 变电站二次系统应设置生产控制区，可按照变电站的电压等级、规模、重要程度以及运行模式差别，按需设置管理信息区和安全接入区，按需将生产控制区细分为安全Ⅰ区和安全Ⅱ区，安全Ⅰ区的安全等级最高，安全Ⅱ区次之，管理信息区再次之，安全接入区最低；
- b) 各安全区应合理规划网络，宜采用不同网段；
- c) 安全Ⅰ区设备可包括监控主机、防误主机、实时网关机、继电保护及安全自动装置、测控装置、PMU 采集设备、采集执行设备等，安全Ⅱ区设备可包括综合应用主机、服务网关机、计量装置、电能质量装置、录波及分析设备以及一次设备在线监测等辅助监控设备等，管理信息区设备可包括视频监控、机器人等辅助监控设备等，不应将属于高安全等级区域的业务系统或其功能模块迁移到低安全等级区域；
- d) 安全区可根据业务特征和功能差异划分安全子区和安全域，明确各安全子区和安全域的边界以及对应的安全防护措施。

6.3 网络边界安全

变电站二次系统的网络边界安全满足以下要求：

- a) 变电站二次系统生产控制区与管理信息区之间存在站内跨安全区数据传输的，边界处应配置

横向单向安全隔离设施；

- b) 变电站二次系统安全Ⅰ区与安全Ⅱ区之间存在站内跨安全区数据传输的,边界处应采用逻辑隔离措施；
- c) 变电站生产控制区的纵向边界处应部署纵向加密认证设施,管理信息区的纵向边界处可按需部署防火墙等逻辑隔离设施；
- d) 变电站二次系统生产控制区不应选用具有无线通信功能的产品,变电站管理信息区辅助监控设备等通过无线网络接入终端和传感模块时,纵向边界处应配置安全接入设备,并采用加密认证措施；
- e) 变电站二次系统安全接入区不应存储重要数据,应使用可信验证措施进行安全防护。

6.4 本体安全

6.4.1 通用要求

6.4.1.1 基础软硬件

变电站二次系统主机、操作系统、数据库、中间件等基础软硬件满足以下基本要求：

- a) 基础软硬件应遵循最小安装的原则,仅安装需要的组件和应用程序,并及时升级安全补丁；
- b) 设备外设接口宜采用物理管控措施保障接入安全；
- c) 操作系统和数据库宜按照“三权分立”原则设置系统管理员、系统安全员和系统审计员,按照职责分工和最小授权原则进行权限划分；
- d) 操作系统、数据库、中间件等基础软件应关闭高危、无关的服务和端口；
- e) 基础软硬件应通过具备网络安全服务资质的国家机构的安全检测。

6.4.1.2 业务系统

变电站二次系统业务软件和装置满足以下基本要求：

- a) 业务软件和装置应对登录用户进行身份标识,用户身份标识具有唯一性；
- b) 业务软件和装置应基于口令、数字证书或生物特征鉴别等技术对用户身份进行鉴别；
- c) 业务软件和装置应满足用户口令复杂度要求,具备用户登录失败处理功能,配置并启用限制非法登录次数等措施；
- d) 业务软件和装置应按照最小化原则,仅开放业务功能相关的服务端口,避免使用高危端口；
- e) 业务软件和装置通信服务接口不应具有运行进程、修改内存等权限,不应通过业务通信接口获得操作系统的执行、写等权限；
- f) 业务软件和装置在业务功能运行过程中应关闭调试端口,防止植入或后门攻击；
- g) 业务装置应采用不同的物理端口进行系统调试和业务数据传输；
- h) 业务软件和装置应采用签名验签等技术措施进行软件版本管控,不应运行未经认证许可的业务程序；
- i) 业务软件和装置应具备软件容错功能、自动保护功能、系统恢复功能；
- j) 站控层主机宜部署恶意代码防范措施,并定期升级和更新恶意代码特征库；
- k) 生产控制区重要业务应优先采用可信验证措施实现安全免疫。

6.4.1.3 通信交互

变电站二次系统通信交互满足以下基本要求：

- a) 变电站二次系统应采用网络通信地址白名单等方式,实现接入对象的合法性验证；
- b) 变电站二次系统应采用数据校验、密码技术等方式保障用户信息、密钥信息等通信交互内容的

完整性和可用性；

- c) 变电站二次系统宜采取加密协议及身份认证等措施,实现重要业务数据交互的安全性;
- d) 变电站二次系统可采取安全认证和加密技术防护间隔层与站控层之间的数据通信;
- e) 变电站二次系统可采取流量分析等技术对业务报文和通信规约进行安全分析、监测及溯源。

6.4.1.4 数据安全

变电站二次系统涉及的业务数据保护满足以下基本要求:

- a) 变电站二次系统应对系统模型信息、保护定值、装置点表、策略配置等重要业务数据进行备份;
- b) 变电站二次系统宜采用国家密码主管部门认可的密码技术保障保护定值、装置点表、策略配置等重要数据在存储过程中的完整性。

6.4.2 站控层设备

6.4.2.1 身份鉴别

站控层设备的控制类操作应采用两种或两种以上的身份鉴别技术。

6.4.2.2 访问控制

站控层设备访问控制满足以下要求:

- a) 设备应对登录的用户分配账户、权限;
- b) 设备应由授权主体配置访问控制策略;
- c) 设备访问控制粒度应达到主体为用户级,客体为文件级、数据库表级、数据表记录或数据表字段级;
- d) 设备应授予不同用户为完成各自承担任务所需的最小权限;
- e) 设备宜支持对重要信息资源设置安全标记功能,并提供基于安全标记的访问控制。

6.4.2.3 安全审计

站控层设备安全审计满足以下要求:

- a) 设备应满足 GB/T 22239 中的安全审计要求;
- b) 设备应具备对审计数据进行查询、分类、排序等功能;
- c) 设备审计记录留存时间应不少于 6 个月。

6.4.2.4 会话管理

站控层设备会话管理满足以下要求:

- a) 设备应具备会话管理机制,当用户处于控制界面并在规定时间内未做任何操作时,应退出控制界面或注销登录状态;
- b) 设备宜具备会话阻断响应功能。

6.4.2.5 采集与处理业务安全

站控层设备具备数据采集和处理业务功能时,满足以下要求:

- a) 设备应只接收被授权对象传输的采集数据;
- b) 设备应只向被授权的对象传输数据;
- c) 设备应对收集的数据进行有效性校验,保证采集数据符合业务设定要求。

6.4.2.6 操作控制业务安全

站控层设备具备操作、控制业务功能时,满足以下要求:

- a) 设备进行手动遥控类操作时,应对用户再次进行身份认证和权限验证;
- b) 设备应对操作控制业务相关的系统模型信息、保护定值、遥控点表等的完整性和合法性进行校验;
- c) 低安全区设备不应通过高安全区的二次设备下发控制指令;
- d) 设备应对业务的操作控制行为进行安全审计;
- e) 设备宜具备对遥控等关键操作的原发抗抵赖功能。

6.4.2.7 运行监视业务安全

站控层设备具备运行监视业务功能时,满足以下要求:

- a) 设备只准许具备权限的用户访问相应的业务模块,监视界面不应有无关信息;
- b) 设备宜采用加密、校验、签名等措施,保证运行监视数据的真实性。

6.4.3 间隔层与过程层设备

6.4.3.1 访问控制

间隔层和过程层设备访问控制满足以下要求:

- a) 设备应对登录的用户分配账户、权限;
- b) 设备应由授权主体配置访问控制策略;
- c) 设备应授予不同用户为完成各自承担任务所需的最小权限;
- d) 配套使用的配置工具软件在连接使用时应进行身份认证,未经认证授权的配置工具软件不应访问设备的任何功能。

6.4.3.2 安全审计

间隔层和过程层设备安全审计满足以下要求:

- a) 审计日志的事件应包括安全性事件和重要业务事件;
- b) 审计日志内容应至少包括以下内容:事件发生的时间、用户/主体、操作内容、事件的结果;
- c) 设备应支持审计日志导出功能;
- d) 设备应具备审计记录容量的管理功能;
- e) 设备宜对审计进程进行保护,防止未授权的中断。

6.4.3.3 会话管理

间隔层设备会话管理满足以下要求:

- a) 设备可具备会话管理机制,当用户在成功登录后超过限定时间内未进行任何操作时,系统可自动结束该用户会话并退出登录;
- b) 设备可具备会话阻断响应功能。

6.4.3.4 采集与处理业务安全

间隔层和过程层设备具备数据采集和处理业务功能时,满足以下要求:

- a) 设备宜只接收被授权对象传输的采集数据;
- b) 设备宜只向被授权的对象传输数据;

- c) 设备应对收集的数据进行有效性校验。

6.4.3.5 间隔层设备操作控制业务安全

间隔层设备具备操作、控制业务功能时,满足以下要求:

- a) 设备进行手动遥控类操作时,应对用户再次进行身份认证和权限验证;
- b) 设备应对相关的保护定值、控制指令等的完整性和合法性进行校验;
- c) 设备应对业务的操作控制行为进行审计。

6.4.3.6 过程层设备操作控制业务安全

过程层设备具备操作、控制业务功能时,满足以下要求:

- a) 设备进行业务功能操作时,应对操作源进行身份认证;
- b) 设备应对控制指令等的完整性和重要标识进行校验。

6.4.3.7 室外终端设备

变电站中布置于室外的辅助终端等设备满足以下要求:

- a) 设备应关闭调试接口;
- b) 设备进行本地及远程升级时,应校验升级包的合法性;
- c) 数据传输宜采取端对端认证、通道加密、数据完整性验证等方式进行安全防护。

6.4.3.8 有线传感器

变电站辅助监控设备等中的有线传感器满足以下要求:

- a) 布置于室外的有线传感器应关闭调试接口;
- b) 传感器宜采用总线方式通信,通过专用的识别码或地址码进行验证;
- c) 基于 IP 地址通信的有线传感器进行本地及远程升级时,应校验升级包的合法性;
- d) 基于 IP 地址通信的有线传感器的数据传输宜采取端对端认证、通道加密、数据完整性验证等方式进行安全防护,也可采取绑定 IP 地址、MAC 地址和端口等方式进行安全防护。

6.4.3.9 汇聚和接入设备

变电站辅助监控设备等中的汇聚和接入设备应满足以下要求:

- a) 汇聚节点与安全接入设备相互通信时,采用国家密码主管部门认可的密码技术实现双向身份认证和数据加密;
- b) 设备支持对变电站二次系统特定的通信协议、端口等进行安全过滤;
- c) 设备具备白名单、访问规则等安全策略功能。

6.5 作业操作安全

变电站二次系统的现场或者远程作业操作满足以下要求:

- a) 变电站二次系统宜对基于网络或存在数据交互的作业行为进行身份认证、权限控制、安全审计;
- b) 变电站二次系统不应通过互联网对生产控制区进行远程作业。

6.6 可信安全免疫

具备可信安全免疫功能的变电站二次系统,可信验证满足以下要求:

- a) 系统引导程序、系统程序、应用程序和关键配置文件等应进行可信验证;

- b) 应用程序的关键执行环节应进行动态可信验证；
- c) 可信验证模块应具备集中管理和异常程序感知监测能力；
- d) 可信根实体应具有国家密码管理局认证的密码产品相关资格证书。

7 安全监测

7.1 基本要求

变电站二次系统安全监测满足以下基本要求：

- a) 变电站二次系统应部署网络安全监测设施，对网络安全信息进行采集、存储、分析、告警等；
- b) 网络安全监测设施宜独立配置，监测功能失效时不应影响业务功能正常运行。

7.2 采集

变电站二次系统网络安全信息的采集满足以下要求：

- a) 采集信息可包括网络安全事件（如异常行为事件、违规操作事件等）、运行状态、网络流量、安全威胁行为、策略与配置等；
- b) 采集的时标宜与变电站二次系统标准时间源保持同步；
- c) 采集功能应支持实时采集、非实时采集等采集模式；
- d) 采集权限控制应遵循最小授权原则；
- e) 采集过程不应干扰业务系统的正常运行。

7.3 存储

变电站二次系统网络安全监测数据的存储满足以下要求：

- a) 数据存储功能应根据不同业务需要设定监测数据存储周期；
- b) 数据存储功能应具备数据备份与恢复能力，监测数据备份周期可根据需要设定；
- c) 数据存储功能应对存储的数据设置访问权限，并对访问行为进行审计；
- d) 数据存储功能宜采取加密技术对重要监测数据进行机密性保护，采取校验机制进行完整性保护。

7.4 分析

变电站二次系统网络安全分析满足以下要求：

- a) 网络安全分析宜包括网络安全事件分析、运行状态分析、网络流量分析、安全威胁行为分析、策略与配置分析；
- b) 网络安全事件分析应支持识别和验证损害被监测对象或造成损失的行为，以及运维等日常操作中的违规行为；
- c) 运行状态分析应支持发现运行状态异常；
- d) 策略与配置分析宜具备安全性校验，以及变更分析、痕迹分析等管理功能。

7.5 告警

变电站二次系统网络安全告警满足以下要求：

- a) 告警功能应支持对安全事件、运行状态异常、网络流量异常、安全威胁行为、策略与配置变更等监测结果的告警；
- b) 告警功能应支持告警信息按需上送至相应的网络安全管理中心；
- c) 告警功能应支持对告警信息的时间源管理。

8 安全处置

变电站二次系统网络安全处置满足以下要求：

- a) 相关人员应结合安全事件告警、系统运行、业务信息等进行告警处置措施的综合研判和决策；
- b) 相关人员应采取可靠有效的隔离、阻断等措施进行有影响后果告警事件的处置，并与相应调度机构进行协同处置；
- c) 相关人员应根据变电站二次系统网络安全应急预案和现场处置方案，采取控制、延缓、阻断等技术措施，正确应对突发网络安全事件，开展网络安全应急处置，最终消除安全风险；
- d) 相关系统宜具备与网络安全管理等其他系统协同实现站内主机设备会话阻断、网络阻断及站内区域边界网络阻断、主子站间通信网络阻断等功能。

9 安全评估

9.1 安全核查

变电站二次系统网络安全核查满足以下要求：

- a) 相关人员应采取现场测评、配置核查、渗透测试等方式进行脆弱性识别；
- b) 相关系统宜具备网络安全基线核查功能。

9.2 安全评价

变电站二次系统网络安全评价满足以下要求：

- a) 相关人员应根据不同安全等级采取相应措施进行网络安全性评价；
- b) 安全评价应包括但不限于资产识别、威胁分析、脆弱性分析、风险分析和安全建议等；
- c) 相关人员应对上线、运行、重大改造等不同阶段开展适应性的网络安全性评价；
- d) 相关人员应对变电站二次系统主要软硬件进行供应链安全评估。



附 录 A
(资料性)

变电站二次系统面临的主要网络安全威胁

变电站二次系统面临的主要网络安全威胁如表 A.1 所示。

表 A.1 变电站二次系统面临的主要网络安全威胁

序号	网络攻击及安全威胁	描述
1	物理空间入侵	非法进入变电站,通过接入物理端口或直接操作站内设备对站内二次系统发动网络攻击等
2	网络空间入侵	非法侵入变电站内外部通信网络,窃取、伪造、截留、篡改变电站二次系统网络通信数据,破坏或者干扰业务的正常运行
3	病毒、恶意软件攻击	变电站二次系统的主机、操作系统、数据库等基础软硬件可能存在的后门或者漏洞,因变电站环境特殊性未及时升级或者更换相关软硬件而长期存在,病毒、恶意软件等容易利用这些后门和漏洞影响二次系统正常运行
4	APT 攻击	变电站二次系统业务软件,特别是嵌入式业务软件的安全性设计不足,在身份鉴别、访问控制、业务逻辑等方面的存在漏洞,黑客等可有针对性的发起 CPS 攻击、勒索等 APT 攻击
5	违规操作	内外部人员违规外联、运维操作不当、安全策略配置不合理、恶意攻击、窃取重要数据等情况

参 考 文 献

- [1] GB/T 37935—2019 信息安全技术 可信计算规范 可信软件基
-

